ORIGINAL

THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | § | |
| | § | |
| V. | § | NO. 3:07-CR-111-K |
| | § | ECF |
| GUADALUPE SANTANA MARTINEZ | § | |

FACTUAL RESUME

In support of the plea of guilty to a one count Information charging a conspiracy to violate 18 U.S.C. § 371 (18 U.S.C. §§ 1029(a)(9) and 1030(a)(5)(A)(ii)) the parties have stipulated and agreed to the essential elements of the offense and the facts.

ESSENTIAL ELEMENTS
18 U.S.C. § 371
(Conspiracy)

First: That the defendant and at least one other person made an agreement to commit the crime of access device fraud (18 U.S.C. § 1029(a)(9), or unauthorized access to a protected computer (18 U.S.C. § 1030(a)(5)(A)(ii), as charged in the information;

Second: That the defendant knew the unlawful purpose of the agreement and joined in it willfully, that is, with the intent to further the unlawful purpose; and

Third: That one of the conspirators during the existence of the conspiracy knowingly committed at least one of the overt acts described in the information, in order to accomplish some object or purpose of the conspiracy.

18 U.S.C. § 1029(a)(9)
(Access Device Fraud)

The essential elements of Access Device Fraud, an object of the conspiracy, are the following:

First: That hardware or software for use on a telecommunications instrument was knowingly used, produced, or trafficked in, and that the defendant had control or custody of, or possessed the hardware or software;

Second: That the hardware or software had been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument, and the defendant knew that it had been configured for the purpose of modifying a telecommunications instrument so that it could be used to obtain telecommunications service without authorization.

18 U.S.C. § 1030(a)(5)(A)(ii)
(Unauthorized Access of Protected Computer)

The essential elements of Unauthorized Access of Protected Computer, an object of the conspiracy, are the following:

First: That the defendant intentionally accessed a protected computer;

Second: That the protected computer was a computer used in interstate or foreign commerce or communication;

Third: That the defendant accessed the protected computer without authorization;

Fourth: That as a result of defendant's conduct, there was resulting damage and loss resulting from a related course of conduct affecting 1 or more other protected

computers aggregating at least $5,000 in value.

## FACTUAL STIPULATIONS

Defendant Guadalupe Santana Martinez stipulates and agrees to the following facts in support of his plea of guilty:

1. During all times relevant to the offense, Martinez lived in the states of Washington and Oregon and conducted his swatting activities from those states. "Swatting" refers to the modification of caller identification information to conceal the true identity of a caller in order to make a fake 911 emergency call, for the purpose of causing a Special Weapons And Tactics (SWAT) response to a specific location.

2. Beginning in or about January 2004, Martinez participated in a telephone chat group with M.W., Chad Ward, Stuart Rosoff, Jason Trowbridge and others. Martinez, M.W., Ward, Rosoff and Trowbridge agreed to conduct swatting calls for purposes of harassing members of the telephone chat group and their families. In order to make the swatting calls, Martinez, M.W., Rosoff, Ward and Trowbridge agreed with each other that members of the conspiracy would make unauthorized access to telecommunication company protected computers to obtain personal identity information of their intended targets, and to use software configured to insert or modify telecommunication services for telephone users in order to obtain free telephone service or discontinue service for telephone subscribers, in violation of 18 U.S.C. § 371. Approximately 15-20 participants in the telephone chat group engaged in the swatting activities including conspirators Martinez, M. W., Rosoff, Ward and Trowbridge.

3. On or about June 12, 2006, Martinez called the 911 emergency services for the City of Cleburne, Texas and identified himself as the father of S.P., and stated that he had shot and killed members of S.P.'s family, that he was holding hostages, that he was using hallucinogenic drugs, that he was armed with an AK47. Martinez demanded $50,000 and transportation across the U.S. border to Mexico, and threatened to kill the remaining hostages if his demands were not met. Martinez placed the call using a voice over internet protocol phone (VoIP) and a spoof card to conceal his true identity, in order to make it appear to emergency services that the call was a true emergency from the address associated with the telephone identification number that had been spoofed. "Spoof" means to tamper with identification information to make it appear genuine.

4. On or about October 1, 2006, Martinez called the 911 emergency services for the City of Fort Worth, Texas and identified himself as the father of S.P., and stated that he had shot and killed members of S.P.'s family, that he was holding hostages, that he was using hallucinogenic drugs, and that he was armed. Martinez told the 911 operator that he would kill the remaining hostages if his demands were not met. Martinez placed the call using a voice over internet protocol phone (VoIP) and a telecommunications facility to conceal his true identity, in order to make it appear to emergency services that the call was a true emergency from the address associated with the telephone identification number that had been "spoofed."

5. Beginning in or about August 2006 and continuing through October 2006, coconspirator M.W. made more than 50 telephone calls to the Verizon Provisioning

Center located at Irving, Texas and obtained unauthorized access to the computers located there and used the access to obtain telecommunications services including caller i.d. blocking and call forwarding. The computers which M. W. accessed were used in interstate and foreign communication, and his unauthorized access violated 18 U.S.C. § 1030(A)(5)(ii). M. W. also used the Verizon computers to initiate new accounts and services for use in concealing caller identification information by the coconspirators, and to terminate services to victims in violation of 18 U.S.C. § 1029(a)(9). M. W. also made unauthorized access to telecommunications provider computers and obtained account subscriber information which was used to identify personal information for targeting victims in violation of 18 U.S.C. § 1030(A)(5)(ii).

6. In or about October 2006, coconspirator M.W. made an unauthorized access to computer equipment of CTS Telecommunications, a subdivision of AT&T, in Grand Prairie, Texas, and used the unauthorized access to modify caller identification information. Subsequently, when Martinez made a phone call directed to the Fort Worth Police Department to make a swatting call targeting S.P. in violation of 18 U.S.C. § 1030(A)(5)(ii), the call transited the CTS equipment in the normal course of call routing.

7. The Verizon computer at the Provisioning Center in Irving, Texas, and the CTS Telecommunications computer in Grand Prairie, Texas were located in the Northern District of Texas, Dallas Division and elsewhere, and were protected computers used in interstate and foreign communications pursuant to 18 U.S.C. § 1030(e)(2)(B).

8. M. W. also provided telephone numbers and pass phrases which were used

to obtain unauthorized access to telecommunications service provider computers with Martinez and others. M. W. and Rosoff obtained the telephone numbers and pass phrases used by the conspirators by various means including the "social engineering" or pretexting of telephone calls to telecommunications company employees, "war dialing", trafficking in pass phrases and access information with other phone "phreakers," etc. The unauthorized access to telecommunications computers obtained by M. W. and Rosoff provided Martinez and other coconspirators with unauthorized telecommunications services. M.W. and Rosoff also used their unauthorized access to telecommunications computers to terminate services to victims, to initiate unauthorized services for themselves and others, and to engage in unauthorized eavesdropping on private telephone conversations in violation of 18 U.S.C. § 1029(a)(9).

9. During the conspiracy, Martinez learned that M. W. was a minor, and even though the telephone chat group was for "adults only," he learned that other minors had participated in the telephone chat group, some of whom were targeted for swatting.

10. As a result of the swatting 911 telephone calls at least two victims received injuries. Martinez was aware that injuries were received by one victim, an infirm, elderly male who resided in New Port Richey, Florida, and that normal municipal activities were disrupted as a result of false 911 calls requiring a SWAT response , *i.e.* road closings, etc.

11. The swatting activities engaged in by the conspirators involved more than 10 victims including individuals, telecommunications providers, and emergency responders resulting in losses of $70,000-$120,000, and resulted in the disruption of the

services of the telecommunications providers which are part of the national infrastructure and emergency responders.

Agreed to and signed this 9th day of April, 2007.

Guadalupe S Martinez

GUADALUPE SANTANA MARTINEZ
Defendant

Charles Bleil

CHARLES M. BLEIL
Assistant Federal Public Defender
Texas Bar No. 00790321
525 Griffin, Suite 629
Dallas, Texas 75202-4520
Telephone: 214.767.2746
Facsimile: 214.767.2886
charles_bleil@fd.org
Attorney for Defendant Martinez

RICHARD B. ROPER
United Stated Attorney
By:

Linda C Groves

LINDA C. GROVES
Assistant United States Attorney
Texas Bar No. 08553100
1100 Commerce Street, Third Floor
Dallas, Texas 75242
Telephone: 214.659.8600
Facsimile: 214.767.2846
Linda.Groves@usdoj.gov